What is claimed is:

1. A method for authenticating a user over a network comprising the steps of:

   a) sending a random number from a remote site to a local site of a user,

   b) measuring a first biometric parameter from said user with a biometric reader,

   c) comparing said first biometric parameter with a previously stored second biometric parameter,

   d) operating on said random number with a math table to create a first cryptogram when a positive match occurs between said first and second biometric parameter,

   e) sending said first cryptogram from said local site to said remote site for comparison with an internally generated cryptogram.

2. A method for authenticating a user over a network as in claim 1 further comprising the step of encrypting said first biometric parameter to form a first encrypted biometric parameter.

3. A method for authenticating a user over a network as in claim 1 further comprising the step of generating a first cryptogram from said random number if said first encrypted biometric parameter positively matches said second encrypted biometric parameter.

4. A method for authenticating a user over a network as in claim 1 further comprising the step of sending said first generated cryptogram to said remote site for comparison with a second cryptogram.

5. A method for authenticating a user over a network as in claim 4 wherein said second cryptogram is generated from a site other than from said local site.

6. A method for authenticating a user over a network as in claim 1 further comprising the step of allowing user access if said first cryptogram matches said second cryptogram.

7. A method for authenticating a user over a network comprising the steps of:

a) sending a random number from a remote site to the site of the user,

b) measuring a biometric parameter from said user with a biometric reader,

c) comparing said first encrypted biometric parameter with a second encrypted biometric parameter previously stored on said biometric reader,

d) generating a second random number when said first encrypted biometric parameter does not positively match said second encrypted biometric parameter,

e) operating on said second random number with a math table to create a first cryptogram when a positive match fails to occur between said first and second biometric parameter,

f) sending said first cryptogram from said local site to said remote site for comparison with an internally generated cryptogram.

8. A method for authenticating a user over a network as in claim 7 further comprising the step of denying user access if said first cryptogram does not match said second cryptogram.

9. A method for authenticating a user over a network as in claim 7 further comprising the step of generating a first cryptogram from said second random when said first encrypted biometric parameter does not match said second biometric parameter.